Transforming Intra- and Interagency Processes through Advanced Models and Simulations: An Information Assurance Model

CARL W. HUNT

Lieutenant Colonel, United States Army
Student, US National War College
US National Defense University
Ft. McNair, Washington, DC
email address: carl.hunt@us.army.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Transforming Intra- and Interagency Processes through Advanced Models and Simulations: An Information Assurance Model	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,National War College ,Fort Mcnair,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**25**	

Transforming Intra- and Interagency Processes through Advanced Models and Simulations: An Information Assurance Model

Abstract: Collaboration among government organizations offers a venue for dramatic improvement in times of national stress. In no technical area is there a greater requirement for collaboration and cooperation than in the field of Information Assurance. Recent innovations in agent-based modeling and other information technologies offer potential for significant progress in improving intra- and interagency processes in Information Assurance and other disciplines. This paper demonstrates how a convergence of Stuart Kauffman's *Patches Theory* with *Agent-Based Evidence Marshaling* can lead to new ways of visualizing and leveraging areas for cooperation among US government organizations and the polices that guide them.

In November 2002, Mr. Gary McKinnon of London, England was indicted for unlawful access and damage to more than 90 US government and private computing systems over a period of 17 months.[1] *McKinnon used a simple but clever technique to by-pass multiple layers of what were thought to be effective computer network defenses that culminated with his access to root-level services that supported numerous mission-critical, although unclassified systems. All of the government agencies that suffered these attacks were subject to federal regulations and policies designed to protect the integrity of the systems under the umbrella of what is known as Information Assurance.*

The investigation revealed that successful intrusion into one agency's computer network ultimately facilitated the intrusion of other agencies' systems through what is known as a "trusted" relationship between systems. The "network" let these organizations down – not simply the electronic communications network, but the network of people, policies and organizations that emerge to produce strength that is greater than the sum of their constituent parts. Although the McKinnon case is hardly unique, it serves as an illustration of the critical requirement for US agencies to cooperate with and support each other in the protection of the United States' critical infrastructure systems. The discovery of even the smallest seam between agencies may lead to exploitation to great disadvantage of the critical infrastructure systems of the United States. This case revealed a dangerous seam that was in fact exploited and resulted in loss of services at a point when it was not decisive to US security—this time.

1. Introduction. Collaboration within and among the most cooperative and mutually supporting government organizations is challenging in times of national and regional stress. Even within the culturally similar organizations which constitute the United States Department

---

[1] See US Department of Justice Press Release, dated 12 November 2002, for more details. This Press Release is located at: http://www.usdoj.gov/criminal/cybercrime/mckinnonIndict.htm. Information explained in the above not provided in the press release is based on the author's personal knowledge as the Commander of the US Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) during the time of the investigation. As noted in the press release, CCIU was a lead agency in the investigation.

of Defense, competition and cooperation jostle each other for ascendancy. More than eighteen months have passed since the attacks on the World Trade Center and the Pentagon, and the relevant agencies at various governmental levels still face challenges to both intra- and interagency cooperation and ultimate success.

Organizations that have worked on behalf of national security in the past, sometimes as competitors for prestige and funding, must find ways to work more closely together in order to preserve national security. These groups must discover and transform the interfaces of cooperation that lead to timely responsiveness to potential and realized emergencies.

This paper examines a novel method of discovering and even exploiting the important interfaces and relationships that affect representative federal-level agencies that must cooperate more closely than ever in national security. The increasingly important field of Information Assurance provides the domain of interest for this research. The methodology proposed, however, has broad application in many areas where multiple organizational interests are at stake and decision-making processes are confounded by competing interests and complex interrelationships among entities.

The model and architecture set forth in this research offers to improve cooperation at many levels and can embrace both government and non-government entities.[2] Information Assurance (IA) cooperation demands transformation and offers a clear example for potential transformational success in many types of organizations and missions.

What is Information Assurance and why is it important? According to the official website of the Defense-Wide Information Assurance Program (DIAP), IA is defined as "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities" (http://www.c3i.osd.mil/org/sio/ia/diap/faq.html). The DIAP is an Office of the Secretary of Defense-level organization that oversees and facilitates DoD-level IA program execution, including the programs of Combatant Commanders, Military Services and Defense Agencies (*ibid*).

This research highlights both intra- and interagency processes that could enhance providing preventative and responsive actions of relevant organizations to threats against security of the information infrastructure of the United States. These organizations include the US Department of Defense (DoD), the US Department of Justice, the US Central Intelligence Agency and the new US Department of Homeland Security. DoD is the target agency for policy enhancement, with the other organizations playing supportive roles in IA strategy development, implementation and enforcement. Success in this critical area enhances transformation across the entire Department of Defense.

This paper also presents a modeling architecture to underpin these new approaches to cooperation. The proposed architecture builds upon recent discoveries about the "information technology" of living systems. The architecture also incorporates new research in the science of

---

[2] These extended areas for research include enhancements to bilateral agreements between nation-states, streamlined planning for the acquisition and integration of new weapons systems, modernized force design in support of military and government transformation, and various complex problems that require cooperation and improvement in effort in the face of dwindling resources. These areas are addressed in the conclusions section of this paper.

networks, emergence and complex systems. The research proposes to adapt and converge a concept Santa Fe Institute scientist Stuart Kauffman called *patches* with a recently developed agent-based modeling system. The union of these concepts will show how building dynamic models of processes that accommodate and harness affinity between organizations can suggest meaningful transition points around which to build cooperation.

A recently proposed model known as Agent Based Evidence Marshaling (ABEM) empowers these patch models to interact and exhibit emergent[3] behaviors that reflect critical lines of inquiry and the transition points (Hunt, 2001). The methodology behind ABEM supports the research reflected in this paper. This research demonstrates how organizational transition points might be discovered and modeled to gain insights about transforming practices and products of the DoD information assurance process in particular and many other organizational and interagency processes in general. This research also shows how modelers may visualize emergent behaviors that can provide commanders and decision-makers insights into complex decision-making tasks.

2. Research Issues.

This research poses the following lines of inquiry:

- Can the intra- and interagency processes within and between critical US security agencies, using information assurance as the primary example, be transformed through advanced modeling and simulation techniques such that foundation processes like coordination and cooperation be improved, and outcomes of organizational interactions become more predictable?

- Can user-level interactions with these models suggest strategies for building emergent policies and procedures that are more likely to be adopted at user-levels in order to provide improved information assurance to DoD systems?

Advanced modeling and simulation techniques, using what are known as agent-based models (ABM), applying network science and Kauffman patches,[4] can provide insights into the DoD's intra-agency and interagency relationships, operations and likely outcomes of interactions of relevant organizations. These insights can be characterized in terms of novel lines of inquiry or responses to inquiry through visual interaction with the models. From these insights, agency leaders can better predict methods to build and streamline actual organizational interfaces that support the interagency process and fashion more effective responses to threats against US national security.

The remainder of this paper focuses in three primary areas:

- A brief presentation of a small representation of agencies that might be modeled in DoD and Homeland Security simulation of emergence models

- A brief overview of network science, complex systems theory (comprised primarily of complexity theory and chaos theory) and relevant modeling research that examines the general interactions of agencies and organizations

---

[3] For the purposes of this paper, emergence is a higher-level behavior that could not have been predicted by observing the behaviors of the individual actors or parts of a system that interacted to produce the observed behavior. Emergence is defined more specifically below. See also Kauffman, 1995 and Morowitz, 2002.

[4] Described below in paragraph 4.

- An introductory description of an architecture and proposed class of ABM that could be suitable for discovering insights about the interagency process

The specific problem addresses emergent governance and interagency cooperation for information assurance, specifically in the vein of developing and adopting IA policies and procedures. An innovative concept of governance through emergent policy rather than centrally-developed policy provides an additional arena for discussion. Figure 1, below, depicts a macro-level view of the model and the agencies and the interactions that might be simulated in a working model based on the proposed architecture.

Descriptions of the agencies proposed for this research are limited, as this research focuses on modeling the interactions of the interagency process and notions of network-based emergent governance.

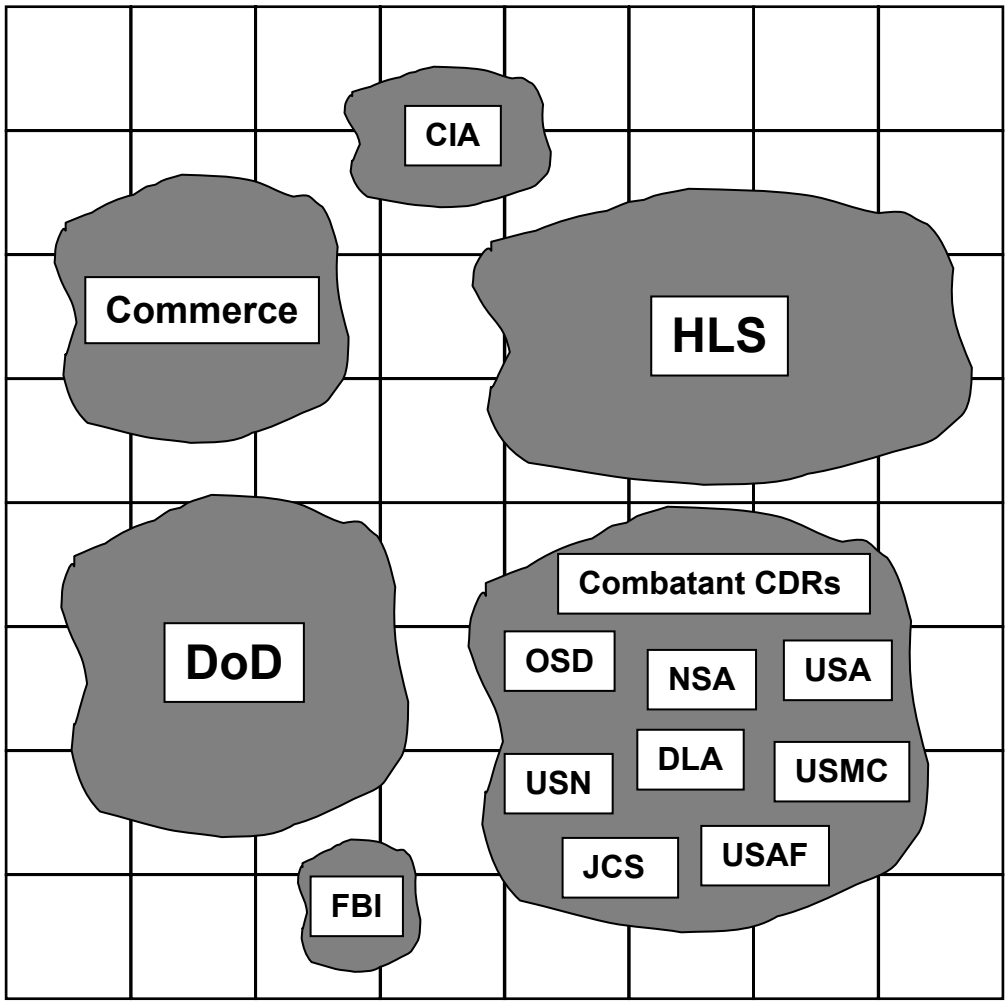

Figure 1. The figure above depicts an 8x8 grid square that notionally represents a portion of the IA community of the US federal government (a DoD IA "landscape"). Some organizations are larger than others, or wield more influence in the conduct of the global body, as shown. More comprehensive research would depict more agencies as well as more accurately attempt to scale the influence each might have. The point behind this depiction is to show the existence of several major players in the proposed simulation of emergence model: Department of Defense (DoD), Department of Homeland Security (HLS), Department of Commerce, Central Intelligence Agency (CIA), and Federal Bureau of Investigation (FBI). A detailed legend for the DoD components is provided in Figure 2. In order to

demonstrate the differences between one "monolithic Department of Defense, there is also a representative patch model of major entities of the DoD that shows several of the major organizations within the larger DoD community. For simplicity, all of these military services are lumped into one patch, although in reality each influences and is influenced by other agencies in different ways. Figure 2, below, breaks out the DoD patch into more detail.

The grid lines in the model above demonstrate possible communication linkages between agencies, and the individual grid squares show areas of influence, some of which may overlap because of mission similarities, cultural likeness, and so on. Not all agencies are directly linked nor does one necessarily influence another, as shown in the model. An actual model would better visualize the complimentary influences of the FBI and the CIA, for example. For the purposes of development of interagency cooperation in the area of IA, linkages between the FBI and CIA may be of less relevance than in other problems. The model above is simply an illustration and not designed to depict actual relationships (see below for an extended example that depicts major actors in the DoD world).

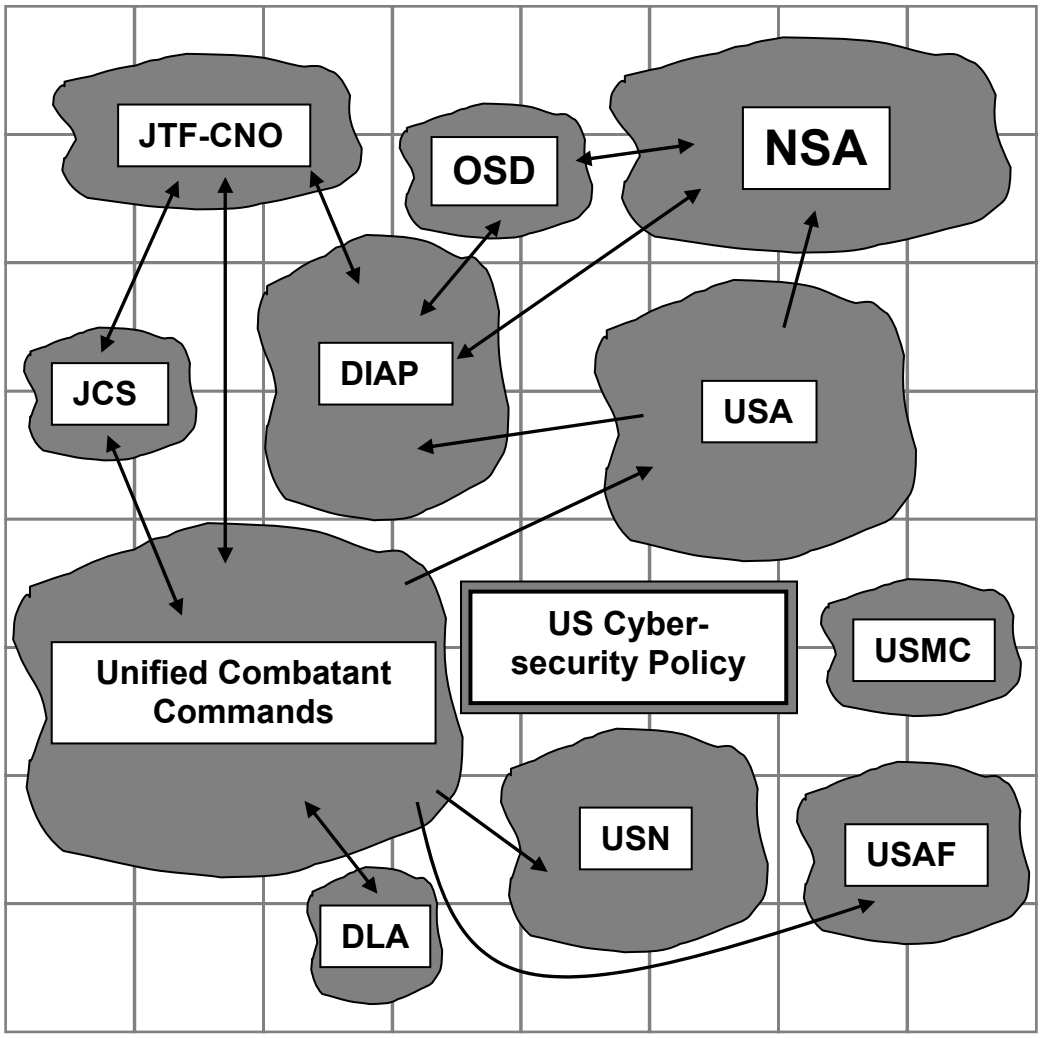

Figure 2. The figure above depicts only the most basic interactive influences of some of the major DoD agencies involved in the simple patch model described in the text. Representative single-pointed arrows indicate a predominant influence of one organization on the other, whereas double-pointed arrows depict a mutually "equal" level of influence upon each organization with neither dominating the relationships. As Kauffman and Morowitz point out, no entity evolves in a vacuum but rather coevolves with its environment, including other entities such as shown in this example. Patches that exert influence that result in change on another patch are themselves changed through coevolution. Changes in one patch can cascade throughout the entire landscape. Coevolution is discussed in detail below.

Note that it is possible to model the effects of policy as well as actors as agents (such as US Cyber-security Policy). The interactions of agent-based representations can feed back into the IA policy planning of DoD which causes adaptation and potential restatement of the problem and policy that addresses the overall IA problem. These issues occur in the real world and the perturbations they pose can cause ineffective use of resources and waste time. Proposed simulations would provide insight and demonstrate courses of action that could more likely predict success. Insights are gained through the visual interactions of patch representations of agencies and the lines of inquiry these interactions pose. Patch-based simulations would suggest better lines of inquiry for leaders to pursue. Asking the right questions help to frame the right problems to solve (Schum, 1994).

Legend of organizations: JTF-CNO – Joint Task Force for Computer Network Operations; OSD – Office of the Secretary of Defense; NSA –National Security Agency; JCS – Joint Chiefs of Staff (and Joint Staff); DIAP – Defense Wide Information Assurance Program; USA – US Army; USMC – US Marine Corps; DLA – Defense Logistics Agency; USN – US Navy; USAF – US Air Force.

This approach to modeling complex organizations is consistent with the tenets of Network-Centric Warfare (NCW). "NCW is offered to provide a rich source of hypotheses to be tested and refined, and a conceptual framework to focus the experiments and analyses ahead" (Alberts, et. al., 119). In other words, NCW, also proposed as a means to transform the US military, provides a valuable cognitive framework for considering experimentation and analysis as core tools for improving the way DoD interacts within itself and with other organizations. The architecture and modeling techniques presented in this paper fully complement what network-centric warfare offers.

3. Selected Relevant Homeland Security Agencies.

The agencies identified in this model must cope with threats against the domestic infrastructure in the particular area of information assurance (IA). US federal policy concerning IA stems from Titles 40 and 47 of the US Code, while Title 18 stipulates criminal procedures for violations of laws related to US Information Assurance policies and capabilities.[5] Under the general guidance of the Director of the Office of Management and Budget, the US Department of Commerce is charged with ultimate responsibility to establish and promulgate policies related to IA (typically referred to in the Code as "Information Efficiency, Security and Privacy," and further enhanced by the various departments under the rubric of Information Assurance).[6]

Title 40 of the US Code requires the establishment of Chief Information Officers in all federal agencies, including the Defense Department and the new Department of Homeland Security (HLS). The Federal Bureau of Investigation, under the Justice Department, and the Central

---

[5] See particularly Chapter 8, Title 47 for Congressional findings about the criticality of telecommunications and information services in the US. Section 1030 (Chapter 47), Title 18, US Code discusses references to IA-related crimes (see also Chapters 119 and 121). The US Department of Commerce, under the general guidance of the Director of the Office of Management and Budget, has overall federal responsibility for computer security and IA (see Sections 1411 and 1441, Title 40, US Code).

[6] Sections 1425 and 1428, Title 40, US Code relate to the establishment of federal interagency support and cooperation, and the creation and responsibilities of the agencies' respective Chief Information Officers. The recent Bush Administration's "National Strategy to Secure Cyberspace" proposes the themes of IA in all levels of government as well as including interfaces to the corporate world and their responsibilities to secure America's linkages through cyberspace (released 14 February 2002). It is possible to trace IA as a governmental responsibility at least as far back as Presidential Decision Directive 63 (May, 1998), where the Departments of Commerce and Defense, as well as the General Services Administration are charged to "assist federal agencies in the implementation of best practices for information assurance within their individual agencies." (See *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, at http://www.ciao.gov/publicaffairs/pdd63.html for more details).

Intelligence Agency also share those requirements, but for the purpose of this research, they are described not so much as interacting agencies but rather as supporters and beneficiaries of the interagency model simulation. The FBI and CIA benefit from or assist in the protection of the agencies that interact in the agent-based model introduced below.[7]

Each department and agency in the US government has placed varying levels of emphasis on IT acquisition and deployment since the "computer age" began. As a consequence, each department has differing levels of sophistication of equipment and access to telecommunications services. DoD, for example, has relied on IT and broadband communications for many years and may have some of the most critical exposures to threats against its information infrastructure – IA has been an important consideration in DoD for a long time.[8]

Configuration control of federal information technology, an integral component of IA, is also a critical concern. Configuration control specifies such things as what kinds of hardware and software may be installed on a computer on a local network, how interfaces to external networks are to be configured and user policies for the agency's computing assets. Misconfiguration often leads to system and network vulnerabilities that can be exploited by criminals, as the above example indicates.[9] Configuration controls are designed to counter such threats and are an inherent part of the IA process.

According to such documents as the 2003 "National Strategy to Secure Cyberspace," however, the federal, state and local governments, as well as precious few commercial enterprises do information assurance and configuration control well (3-5). Massive interconnections between all of these systems (such as through the Internet) make effective policy development and implementation extremely complex, but an imperative nonetheless.

The challenge is to fully understand the enormity of the problem and to build effective models and simulations that not only help to visualize the challenge but suggest ways to offset threats and build better IT infrastructures. Modeling interagency cooperation and policy development is an important first step.

Figure 2, above, is an early attempt to visualize some of the most basic interactions of relevant DoD players in this problem domain without the benefits of an actual agent-based model. It suggests that there are policy and governance disconnects that may be visualized and overcome in order to make DoD IA more effective. The core of this research includes the theory and architecture that can link the IA problem to simulation of emergence models that may provide insights towards solutions.

4. Complexity Theory, Patches and Agent-Based Models. It is useful to be familiar with some basic premises of complex systems theory and emergence in order to understand how to construct and comprehend the outcomes of simulation of emergence models. In the case of this research – the attempt to enhance DoD IA with new capabilities to model and visualize complex relationships between policy, governance and technology – it is important to be aware of the basic theories about complexity and chaos, networks and agent-based models, including patches.

---

[7] In such a sense, the FBI and CIA are in fact part of the interagency process described, if only implicitly.

[8] See for example the roles and responsibility of the Office of Secretary of Defense's Assistant Secretary of Defense for Command, Control, Communications and Intelligence, who also serves as DoD's Chief Information Officer (http://www.c3i.osd.mil/). Each of the military services has subordinate counterparts to this office.

[9] This also includes international criminals, commercial spying and foreign espionage.

Complexity Theory. There are several ways to define complexity in relation to complex systems theory, but they typically incorporate two formalized systems of study: chaos theory and complexity theory. The notions of emergence and coevolution are also important in understanding how complex systems work individually and can interact effectively with each other. These concepts help to recognize the power of agent-based modeling and simulation.[10]

Management consultant and Industrial College of the Armed Forces lecturer Irene Sanders provides succinct definitions of chaos and complexity theories in her current lectures and book:

> *Chaos theory describes how a sensitive dependence on initial conditions contains the potential for change through (what is known as) the Butterfly Effect.*[11] *Complexity theory describes how order and structure arise through the process of adaptation set in motion by new information, which tips the balance and pushes the system into a chaotic episode…complexity theory incorporates and depends upon the details of chaos theory…(while chaos theory) is the mechanism through which change is initiated and organized. It is the way the world creates the rich diversity that we see all around us.* (Sanders, 69-70).

The study of complexity may also be likened to the study of life and the environment in which life exists. It deals with how living and "non-living" environmental entities interact with, or coevolve with each other to produce the behaviors that can ultimately be observed. Organizations, particularly those composed of people, also produce complex and often unpredictable behaviors; some of these behaviors lead to innovation. Several complexity authors, including Sanders and Kauffman, speculate that a rich transformation zone for innovation lies in a notional space called the *edge of chaos*.[12]

To change an entity that is frozen into an ordered state, according to Sander's definition, it may be necessary to unfreeze the entity through the introduction of some sort of chaotic phenomenon. If it were possible to control such changes (such as innovation) it would be desirable to have a launching pad or transition zone to observe and tweak these introductions of chaotic behavior to avoid a cascade into system-wide uncontrollable behaviors. The so-called edge of chaos seems to identify this "place" for experimentation. It would likely not be possible to accurately predict the outcomes of the introduction of these chaotic tweaks, so novelty and innovative behaviors may thus be thought of as *emergent*.

Emergence is a basic component of complex systems theory that requires additional explanation – it is the foundation of the modeling techniques that follow. The study of emergence "tries to generate the properties of the whole from an understanding of the parts," and thus offers the potential for deeper understanding of complex systems, notes George Mason University biologist Harold Morowitz (14). Emergence reflects new levels of organization or structure that could not

---

[10] Agent-based modeling is defined in greater detail below.

[11] The *Butterfly Effect* refers to the way small changes in what were once thought of as linear systems can produce unpredictable and sometimes wildly fluctuating behaviors in systems. Chaos theory pioneer Edward Lorenz is credited for posing the example that a butterfly flapping its wings in one part of the world could ultimately be responsible for a hurricane or tornado somewhere else in the world. See Sanders, pp. 53-61.

[12] The *edge of chaos* is said to exist in a transition state between rigid order and a chaotic condition (See Kauffman, 1995, pp. 26-29, and compare with Sanders' discussions about the interfaces of chaos and complexity, in the paragraph above). The discussion about Kauffman patches, below, speculates more about this environment.

have been previously predicted from observation of the individual parts of the organization alone (Hunt, 11). The emphasis is thus on novelty and discovery of properties not deducible from observation of the component parts.

In a sense, complexity is part of the definition of emergence and emergence is part of the definition of complexity. These definitions are manifested in the difference between complex and complicated – words that are often but incorrectly substituted for each other. There is a distinct difference between something that is complex and something that is complicated. Paul Cilliers notes the differences succinctly:

> Something that is *complicated* can have many components, and can be quite intricate, but the relationships between the components are fixed and clearly defined…Something that is *complex* on the other hand, is constituted through a large number of dynamic, nonlinear interactions…complex things have emergent properties, complicated things do not. (Cilliers, 41).

Cilliers points out that when the relationships between components of complex systems are broken (e.g., in disassembly), "the important characteristics of a complex system are destroyed;" this is not the case in complicated systems which often require analytic breakdowns to understand system behaviors (*ibid*.). Emergence is the key difference between complex systems and complicated systems.

Coevolution is the final component presented in this brief overview of complex systems theory. Kauffman notes that evolution is really coevolution in the sense that entities or systems do not evolve in a vacuum. In a Darwinian sense, evolution is an adaptation to some external stimulus that forces change to occur in order to survive or be in position to improve one's standing on the "food chain" of life (Kauffman, 222).[13] Changes in one system typically stimulate change in adjacent systems or environments – the essence of coevolution. Kauffman's ideas about patches closely follow this notion.

Patches. Stuart Kauffman's patches model follows the ideas he presented in his original *NK* landscape. His *NK* landscape model evolved from the initial work he did in what he called Random Boolean Networks, another innovative application of network theory (1993, 182).[14] Random or "Disordered complex Boolean networks, it has turned out, exhibit three major regimes of behavior: ordered, complex, and chaotic" (183). The structures and linkages Kauffman describes in this earlier work set the stage for his later notions about patches.

According to Kauffman, patches are simply another way to classify what all life does in evolutionary systems. Adages such as "act locally and think globally" and "all politics are local" reflect how humans have intuitively thought of patches, absent the benefit of reading Kauffman. Patches are a visualization of Stuart Kauffman's *NK* landscape model (also built upon his random Boolean network ideas), where the behavior of an object *N* is influenced by its connections to *K* other objects. There may be many objects *N*; and, each *N* object may be affected by varying *K* other objects (1995, 173). Recall the visualizations in Figures 1 and 2 as they depict simple models of patches, or organizations, and consider them as *NK* landscapes.

---

[13] Morowitz goes even further, noting that "all evolution is coevolution," (183).

[14] Boolean functions are essentially algebraic expressions of premises rather than numbers. See Devlin, page 58-61.

The possible combinations of connections between nodes in a typical "network" of DoD organizations could be daunting. Kauffman proposes that patches are a way of avoiding combinatorics by finding solutions that are good enough rather than the "best." He suggested patches as a search tool similarly to the way he defines evolution as a search procedure (1995, 248) – by empowering a local organization to develop in ways that optimize its own potential, the global organization can grow and mature in ways not foreseen.

This is comparable to the way an ecosystem might flourish as the constituent parts develop in "greedy" ways subject to the loose constraints of the overall ecosystem. As Kauffman explains in *At Home in the Universe*:

> *The basic idea of the patch procedure is simple: take a hard, conflict-laden task in which many parts interact, and divide it into a quilt of non-overlapping patches. Try to optimize within each patch. As this occurs, the couplings between parts in two patches across patch boundaries will mean that finding a "good" solution in one patch will change the problem to be solved by the parts in the adjacent patches…Patches, in short may be a fundamental process we have evolved in our social systems…to solve very hard problems* (252-253). (Refer to Figures 1 and 2 for simple visualizations.)

Thus, breaking the problem into smaller chunks (the reductionist approach), allowing for appropriate couplings (such as networks, or the common thread of the commander's intent) and then allowing the component parts to solve for their local "optimal" solutions, generates perturbations that percolate throughout the entire organization. These perturbations tend to unfreeze localized locked-in behaviors and push the organization to move to higher planes of rich complexity as the overall organization attempts to satisfy more of the component parts' individual issues that are linked to other component parts' solutions through boundary communications.[15]

No solution is arrived at in a vacuum in such an environment, while the organization does not have to engineer the "perfect" solution from the beginning. The solutions emerge based on component interactions, an identifiable parallel to the intra- or interagency process.[16]

Patches do not solve problems as much as they visualize the issues associated with solving the right problems. It is obviously helpful, but typically impossible, to specify the right problem in the beginning. "Misspecification is…endemic," notes Kauffman, based on his personal research with management experts. Leaders rarely define the right problem to solve in the first place if for no other reason than incomplete information. "We must learn how to learn in the face of persistent misspecification," writes Kauffman (1995, 266-267). Patch theory is his contribution to resolving the dilemma posed by incorrectly specifying the problem originally, while avoiding the combinatorial explosions that can occur when trying to find optimal solutions among complex interactions of multiple organizations.

Solutions to these classes of complex problems reside in a regime known somewhat scientifically as the edge of chaos, as noted above.[17] Recall that Kauffman in his description of Boolean

---

[15] The concept of simulated annealing also generally describes a variant of the patch model (see Kauffman, 1995).

[16] A very basic understanding of fitness landscapes, a model for visualizing improvements or declines in fitness of an entity (or even policy), is useful for comprehending Kauffman's NK and patches models, but is beyond the scope of this paper. See Kauffman, 1995, and Morris, 1999 for more details.

networks noted that there were three states possible: ordered, complex and chaotic (1993, 183). His term "complex" in this sense aptly describes the edge of chaos.

The edge of chaos exists in a transition state between rigid order and a potentially inscrutably chaotic condition. In simplest terms, chaos is unpredictable and perhaps impenetrable, while order is a state of extreme stability or inflexibility. This definition does not seek to denigrate either extreme as both can be useful in certain conditions.[18]

The edge of chaos is a state, however, where novelty can be discovered and appreciated; within this state, new policy and organizations can emerge to dampen the perturbations that often affect agencies, as the new policy pushes the organization(s) toward more order. Adaptation tends to occur at the edge of chaos, for example, in an area that is not quite ordered and not quite chaotic. This is the essence of the patch model.[19]

It is worth revisiting Alberts' thoughts concerning Network-Centric Warfare as a "rich source of hypotheses to be tested" (119). NCW and the edge of chaos philosophically share a common tenet: both serve as a setting for experimentation and adaptation. Sanders suggested that new information "tips the balance" of order, potentially pushing the system into a chaotic or non-equilibrium state (69), which then tends to cross over the notional edge of chaos as it transitions from one state to the other.[20] From Alberts' general description of the transformative nature of NCW, it seems the network offers similar functionality. NCW provides a facilitating environment for information flow and the hypotheses that emerge from unresolved issues to transition from state to state.

In a strong sense, the emergent architectures that would support Network-Centric Warfare provide adaptive surroundings for the information that supports the warfighter to transition from rigidly ordered states, such as found in structured databases, to relatively disordered states where self-organization could foster greater creativity in problem-solving. The question then is "can the commander sufficiently control or shape the network so that it nourishes both the flow of information and the emergence of novel but testable hypotheses?" Can new insight be gained from the same information viewed in different ways? Network theory also says something that would address this important question.[21]

Phase Transitions and Transformation. The notion of a phase transition is important to understand how organizational entities such as patches can ultimately produce models of organization or policy. Simply speaking, a phase transition describes the change of state from one regime to another. A common example is the change of state from ice to water to steam, which is also a limited example of Kauffman's ordered, complex and chaotic states from his descriptions of random Boolean nets. As frozen water molecules are heated and speed up

---

[17] See generally Kauffman, 1995.

[18] Compare to Sanders' definition above. The simple definition shown here simply indicates the contrast between chaos and order. Relationships in a chaotic state appear to be loosely coupled, if at all, while relationships in an ordered state are frozen in place and require some sort of new information to break free (as Sanders indicates).

[19] See also Kauffman, "Escaping the Red Queen Effect," The McKinsey Quarterly, 1995, for an interesting parallel analogy to Adam Smith's "Invisible Hand."

[20] Compare to Kauffman's thoughts about "disordered complex Boolean networks," described above, in which he suggests that complex Boolean environments possess three regimes: "ordered, complex, and chaotic".

[21] Not only does network theory speak to this question, but so does Kauffman's invention of the technology graph. The technology graph is also the backbone for Agent Based Evidence Marshaling, as described below.

enough to thaw into liquid water, enough of the molecules "convert" as it were so that the water is liquid rather than frozen or rigidly ordered. The same description applies to the way a collection of liquid water molecules dissipates into the more chaotic state of steam.

When enough nodes (or patches) in a network change state with a resultant new behavior, a phase transition may have occurred. This behavior may be complex (due to emergent phenomenon) or simple (e.g., directly traceable through cause and effect relationships). Models that are looking for emergence may be able to identify states that lead up to the phase transition, thus potentially arming commanders and analysts with tip-offs that a change of state is imminent. US military commanders also call these tip-offs "indications and warnings."

Traditional engineering, management, and organizational behavior approaches tend to perceive all global behavior events as cause and effect-based, and thus tend to prescribe solutions suitable to simple (e.g., non-complex) behaviors. The same applies to policy development and implementation. Alberts (15-16) notes the friction between engineering and innovation, calling for a coevolving fusion of engineering and innovation.

Traditional engineering approaches can ignore the innovations of emergence, phase transitions and complex adaptive systems behavior. Similarly, military planning that tries to foresee and accommodate every contingency may miss what could happen in the seams between the "foreseen". While these concepts in themselves may or may not directly cause behaviors, they are valuable ways of thinking about observed behavior and deducing the linkages and interactions of components that produced the behavior. Broader thinking is truly the "hidden agenda" when considering emergence.

Understanding emergent behavior should go a long way toward understanding how to bring about transformed organizations and behavior. "Transformation," notes Alberts "is a process of renewal, and adaptation to environment…Change and human adaptation are always the essential ingredients in transformation" (vii). Just as the notion of an edge of chaos relative to transformations seems relevant, phase transitions and transformations also appear to have a great deal in common. They reflect changes in state, often the results of some sort of "adaptation to environment."

Also, just as it is unclear whether or not transformation can be managed (Alberts, *ibid*.), it remains largely unanswered as to whether phase transitions can be brought about or "shaped" on demand. More often, phase transitions may "sneak up" and set off cascades of unpredictable behaviors or consequences, such as the events that led up to and included the attacks of 11 September 2001. Agent-based models begin to provide a way to move towards simple solutions for complex problems.

Agent-Based Models. ABM are models of real-world environments that allow for leaders to visualize the relationships between entities. Each entity reflects agency, or self-directed behavior that interacts in an environment suitable to reflect behavior. These behaviors may be so finitely pre-specified as to preclude novelty, or, towards a more meaningful outcome, sufficiently programmed to allow for emergence to occur. Agents are software representations of real or possible entities that are constructed to reflect possible or potential outcomes of interaction. Rules are embedded in the simulation to provide realistic boundaries for emergent behavior.

A significant advantage of agent-based models is that the leader can gain visual insights into possible futures that encompass multiple perspectives rather than singular projections of

subjective notions of cause-and-effect. In other words, ABM can help a leader break out of equilibrium thinking when faced with an unstable, highly dynamic environment. These simulations make it possible to search for non-equilibrium areas that arise from equilibrium states of organization and visualize the transition points between states where leadership decisions have the most leverage.

Robert Axelrod considers agent-based modeling as "a third way of doing science" (where induction and deduction compose the other two inference methods; Axelrod, 1997, 3). He also cites agent-based modeling's goal as "enrich(ing) our understanding of fundamental processes that may appear in a variety of applications" (5). In this sense agent-based modeling is experimentation for the masses, helping to turn many towards analysis and synthesis than currently do it now. It is most certainly a tool, but a tool that can change the way we think and formulate inquiry about the world we face.

Agent Based Evidence Marshaling (ABEM): an architecture to resolve complex problems through natural systems approaches. The Agent Based Evidence Marshaling (ABEM) model harnesses this proposed flow of information to lead from the origination and initial storage of information through the process of discovery to a process that empowers articulation and defense of arguments that support commander-driven decision-making.

ABEM research (as described in Hunt, 2001) blends a manual mode of evidence (or information) organization developed by David Schum and Peter Tillers (Schum, 1999) with an agent-based modeling environment known as a technology graph, developed by Stuart Kauffman (2000, 222).[22] Organization of evidence, or information objects, on the graph setting of an economic web enables what is essentially a negotiating environment for acquiring or trading information with other objects in ways that spread the potential for discovery of new information.

"Evidence" is a semantic convenience that encompasses any item of information that tends to persuade an investigator or decision-maker to further prove or disprove any hypothesis or previous frame of thought. Observations of evidence from the real-world are translated into ABEM as object-oriented packages of information.

These object-packages can facilitate self-organization of the observations in ways such that they pose questions to each other as well as to a human investigator. The learning that takes place within each evidence object empowers the development of powerful data structures capable of recombination into new questions, increasingly refined hypotheses and even the deduction or nomination of new evidence that would improve decision-making or implementation (Hunt, 2001). Figure 3, below, depicts the basic architecture of ABEM.

---

[22] According to Kauffman (2000), a technology graph is "A set of primitive parts and the transformation of those parts into other objects." This graph-based concept empowers object-oriented representations of real-world information to combine and recombine into novel or transformed objects that may better exploit their information environment. In this sense, the agent-based model allows for exploration (or discovery) within an environment while technology graphs allow for exploitation of the environment simultaneous to the exploration process. ABEM combines both concepts into a single agent-based modeling virtual world, transforming evidence and initial questions into new (or deduced) evidence and working hypotheses. More advanced iterations of ABEM, as developed by Jim Herriot and Bruce Sawhill (*ibid*.) allowed for self-testing of hypotheses in situations where evidence was consistent and non-contradictory. They have also experimented with inconsistent and contradictory evidence, although this work has been clearly more challenging.

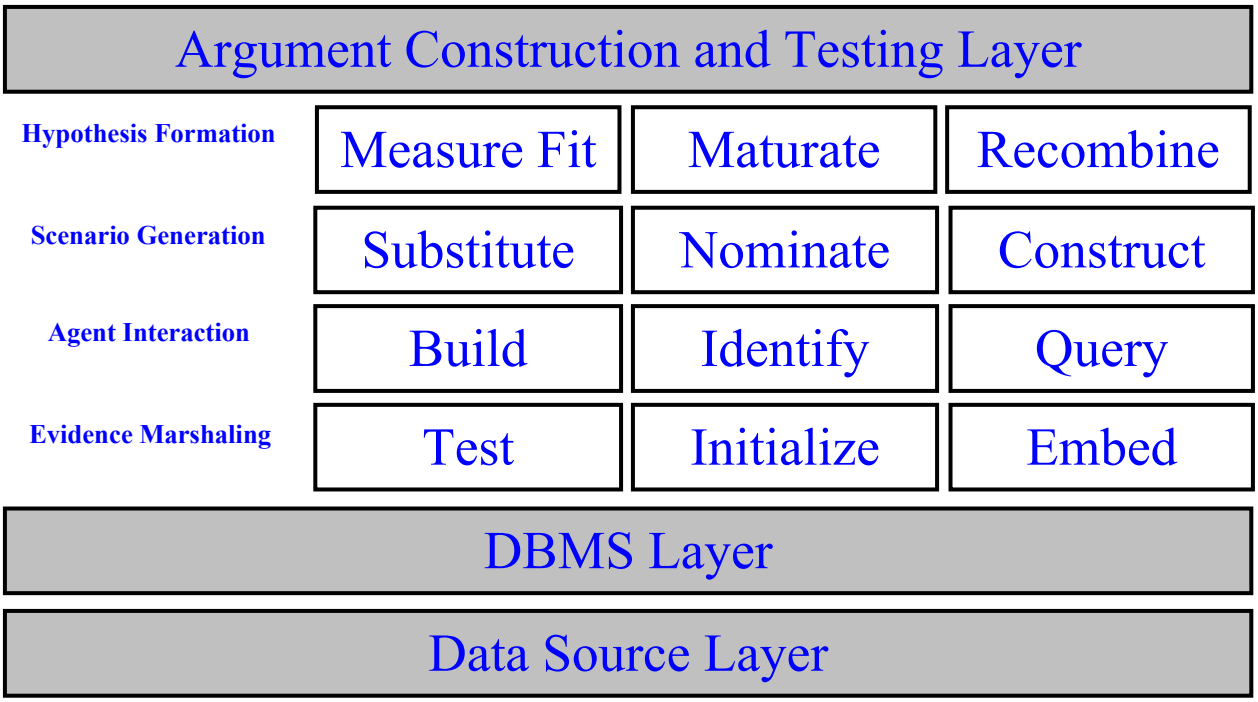

Figure 3. The ABEM Architecture. This drawing depicts relevant processes that influence the transmittal of information from one layer to another as well as between processes, as described below. The goal of ABEM is to empower information extracted from various data sources to mature through a self-organizing process that eventually results in valid and cogent arguments that may be articulated coherently to a decision-maker. The Evidence Marshaling, Agent Interaction and Scenario Generation Layers are described briefly below and in detail in Hunt, 2001. The higher layers, Hypothesis Formation and the Argument Construction and Testing Layers are being researched by Stuart Kauffman, Bruce Sawhill and Jim Herriot (as proposed and discussed in Kauffman, 2000).

A brief description of the ABEM architecture begins at the Data Source Layer. This layer represents various existing and emerging methods for storing and processing data inputs such that information content can eventually be extracted. At this stage, data has not been processed or analyzed in great detail, but only collected and tentatively "organized" in traditional database formats. Processing and manipulation of data for more extensive analysis and transfer to compatible record extraction occurs at the DBMS (Data Base Management System) Level.

The Evidence Marshaling Layer captures the original work of David Schum and Peter Tillers in their *MarshalPlan* system (Schum, 1999). The components of this layer include testing, initializing and embedding information for the remaining layers. Testing deals with the first point at which an investigator or analyst thinks of information as evidence. It includes an examination of the candidate evidence item's credentials such as relevancy and reliability to ensure the information is suitable for use as evidence.[23]

Once found to be acceptable, the system accommodates the Initialization of the evidence, which includes verifying relevant details and extracting suitable components of it to be used in tuple

[23] For a detailed discussion on the credentials of evidence see Schum, 1994.

format, the *lingua franca* of ABEM agent communications.[24] Finally in this level, ABEM Embeds the initialized evidence into a form suitable for tuple-based communications and agent-based learning that occurs in the ABEM simulation.

The next major ABEM architecture level is called the Agent Interaction Layer. The first component is the Build process, which accepts the marshaled evidence observations and constructs object-agents from these observations. It is at this point that evidence observations enter the object-oriented world of technology graphs and can become part of the transaction-based movements the tuples accommodate. Next is the Identify component. In this process, ABEM tuples are used to satisfy what appears to be a vast hunger for self-knowledge on the part of ABEM agents. Through this subjective process (accompanied by the substitution capability described below), agents actually learn a great deal of information about not only themselves but other agents who become important to them.

Working hand-in-hand, the Identify and Query components reflect the learning process of ABEM agents. The questions agents ask each other are based on attempting to build a more complete space-time vector for themselves, hence the advantage of coding ABEM tuples in terms of space and time for this iteration of the model. Without "understanding" where this space-time vector might logically terminate, the agents nonetheless seek information about where they may have been inside their virtual world, including tracking space-time vectors of other agents once they "infer" some relationship to themselves.

Agent inference is an important concept of the ABEM architecture and working models. The Scenario Generation Layer empowers inference and learning on the part of the agents. The first sub-component of the Scenario Generation Layer is Substitution. The concept of Substitution is related closely to Kauffman's description of substitutes (and complements), as discussed in Kauffman (2000). It is also related to what artificial intelligence pioneer Marvin Minsky calls "multiple representations" when expressing what he calls "commonsense thinking" (Minsky, 71). As Minsky writes:

> If you understand something in only one way, then you scarcely understand it at all because when something goes wrong, you'll have nowhere to go. But if you use several representations, each integrated with its set of related pieces of knowledge, then when one of them fails you can switch to another. You can turn ideas around in your mind to examine them from different perspectives until you find one that works for you. And that's what we mean by thinking! (Minsky, 67).

ABEM substitution does not pretend to empower machine thinking, but it does allow the analyst to observe data representation from different perspectives as the object-agents seek substitutes for themselves during the query process. Figure 4 depicts an ABEM screenshot where a substitution tuple message both asks and responds to an agent query.

---

[24] Tuples in ABEM are patterned after David Glertner's pioneering work in message passing between database objects – they are essentially fields or "rows" from a database, in the way that Glertner introduced them. Tuples were adapted for use in the ABEM environment by Bios Group Scientist Jim Herriot (Hunt, 2001), who built in the time-space orientation for message passing. Examples of tuples in action appear in the ABEM in Figure 5.

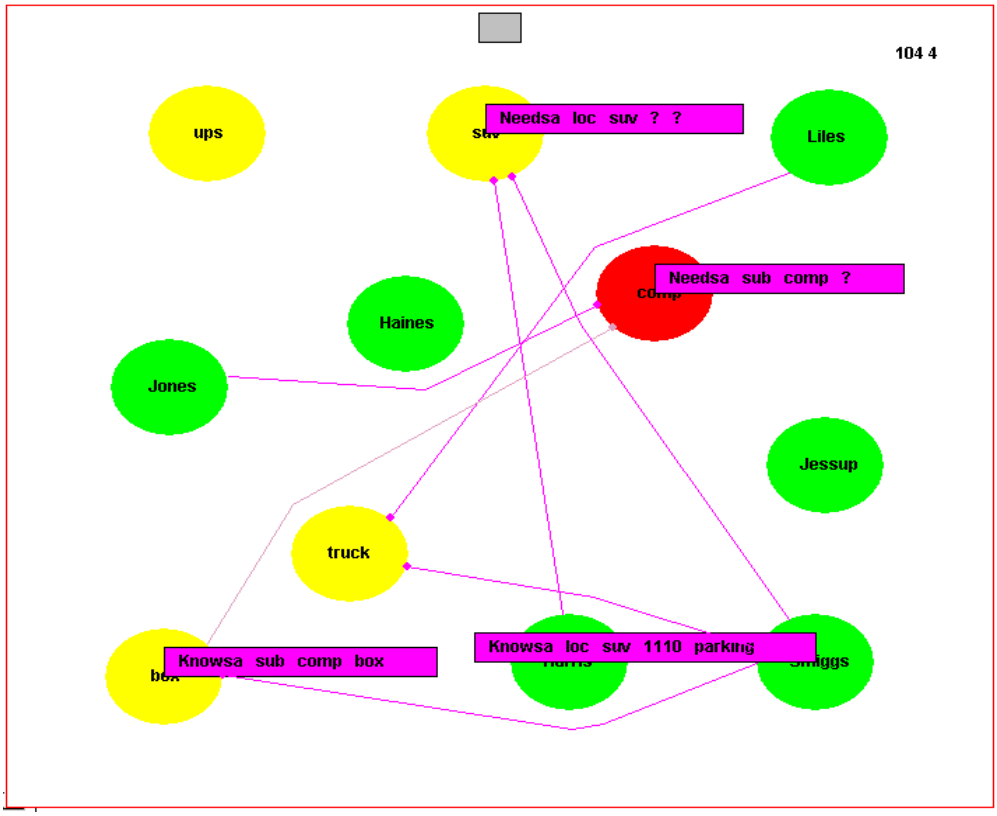

Figure 4. ABEM screenshot. This screenshot from an ABEM simulation depicts the two major tuple-based queries that ABEM agents utilize. At the top center portion is the "SUV" agent asking the "Harris" agent if it knows a location (called loc in the tuple) for itself (an agent-based representation of a sport utility vehicle; "Harris" is an agent-based representation of a witness to a crime). The two question marks concluding the query are placeholders asking for information that pertains to time and space, respectively. The second type of ABEM tuple-based query is a substitution query as described above. In this instance the "computer" agent in the middle right of the screenshot is asking the "box" agent if it knows if there is a substitute for it (called "sub" in the tuple). The "box" agent responds back to the "computer" agent that it knows that it (box) can be a substitute for the computer. In the case of this particular simulation, the box is capable of holding (or concealing, in the case of a deception) the computer. In other words, where the "box" agent is in space and time becomes an important bit of knowledge for the "computer" agent that is trying to piece together its own time-space vector. In Minksy's terms, the "computer" agent can have "multiple representations" in what would otherwise be a very linear vector. Agent-based models such as ABEM empower analysts to visualize outside the traditional vectors that appear grounded in obvious cause-and-effect relationships. These types of models help decision-makers test hypotheses that don't neatly fit within conventional relationships among objects.

The next component is the Nominate process. Quite simply, the nomination process of ABEM involves the introduction of a new, yet to be discovered evidence object that helps to hold a place for potential evidence. In his description of the *MarshalPlan*, Schum referred to these placeholders as "gap fillers" (Schum, 1999). The ABEM process of nomination serves as the "temporary" filler until the relevant evidence observation is made. Nomination empowers deduction and potential prediction of what to look for and even where to find it.

Construction is the final component of the Scenario Generation Layer. In the current implementation of ABEM this is an analyst-driven intuitive process that results in the

construction or development of likely scenarios of what transpired or could transpire based on the interactions of ABEM agents. Out of scenario generation, the analyst builds and tests hypotheses (or questions) about the evidence or environment that has not yet been made clear. Scenarios provide glimpses of what is possible and what needs to be known to become more certain about the matter in question.

There are two remaining layers in the ABEM architecture. Although the Hypothesis Formation Layer is not well developed at this point, it is clearly an important direction in which to extend this work. Its three components include measurements of fitness, maturation and recombination. By providing emerging and developing hypotheses unique methods of identification similar to the genomes of living systems, hypotheses can potentially "recognize" each other and what may be important to their existence and growth. Tuples and agents are components of these genomes. Genomes offer constructs which can be measured and positioned in hierarchies that demonstrate fitness. This is the thrust of the theory behind fitness measurement in ABEM.

Maturation is simply a process of empowering interaction and nurture through the movement of evidence and hypotheses around a virtual ABEM landscape. The proposed ABEM landscape provides sustenance in terms of evidence and inference factors that assist in maturing the developing hypotheses (Hunt, 2001). Recombination is a proposed feature that allows existing hypotheses to "collide" and swap their equivalent "genetic material" in ways that evidence items may be transferred in context by means that had not been observed in the real world. Both of these features are derived from the benefits of the simulation capabilities of agent-based models like ABEM. While little modeling work has been done in this layer, great potential for discovery exists by extending the ABEM work in this direction.

The final part of the ABEM architecture is Argument Construction and Testing Layer. No single piece of evidence stands on its own. Evidence must be considered in context with other pieces of evidence and the lines of inquiry they suggest. To convince a decision-maker about the effective use of evidence an argument must be successfully presented and debated or tested. Decision-makers must understand the arguments analysts pose to them. The evidence analysts seek to support their arguments are strongly influenced by the order in which they have previously learned information; recall the original quotation at the beginning of this paper. Presentation and testing infuses the rigor of the scientific method into decision-making. Schum (1994, 1999) lays out both theoretical and practical considerations for constructing and testing arguments that would be essential to incorporate into more sophisticated versions of ABEM.

In summary, Agent Based Evidence Marshaling is a fusion of Stuart Kauffman's Technology Graph model and David Schum's Evidence Marshaling model. The technology graph provides a network-based linkage model to empower agent emergence and growth while the evidence marshaling model inspires the acquisition, maturation and generation of evidence and hypotheses. This convergence of models has two main objectives: inspire decision-makers to seek more productive lines of inquiry, and fashion and test arguments in novel ways that reflect living systems-based processes of self-organization.

Borrowing another Kauffman model, patches, and infusing it with the potential power of ABEM introduces dynamic new ways of modeling and testing organizational growth and development both in terms of designing and staffing organizations and in testing the policies and methods of governance of complex organizations. From these proposals comes a prospective modeling

environment for discovery about complex interagency processes in general and the information assurance policy setting in particular.

5. Modeling the Interagency Process through Emergent Simulations.

In terms of vulnerability of networked systems, an organization's computer networks are basically as strong as the weakest system in the network, including the people in that network. Configuration control policies as part of the IA umbrella are designed to prevent vulnerabilities by enforcing baseline rules as to what might be placed on government networks in the first place, and create the hardware basis for a more trusted environment for information processing.

In spite of a common regulatory baseline, however, not all federal agencies do configuration management the same way. Organizations often don't even have commonality of equipment intra-organizationally much less across the federal government. The challenges are enormous in such an environment of mixed configurations and local policies of exception.

Agent-based models, applying Kauffman's patch theory, could help solve this challenge. To be sure, this paper does not propose to use simulation of emergence models to support the mechanical process of configuration control, although it could be useful to comprehending the complex issues involved. The purpose of this research is to propose how to use patches and ABM to fashion appropriate policy that facilitates interagency and organizational interaction, governance and cooperation that would improve the global state of IA for DoD and the entire federal government. Visualizing the complexity and potential outcomes of developing meaningful interagency policy, as well as discovering new, more useful interface points between organizations is an area ripe for the potential benefits of agent-based models.

US law embodied in the US Code discussed above charges the Department of Commerce as a guiding agency in coordinating and promulgating IA policy. According to the new Department of Homeland Security's initiating documents, DHS will be responsible for Information Analysis and Infrastructure Protection among other functions. These two agencies should coordinate with the Department of Defense to develop consistent information assurance and configuration control policies. These three agencies are thus candidate patches for an emergent simulation of interagency IA policy development.

As pointed out earlier, however, the FBI and CIA are potentially both supporters and beneficiaries of the outcomes of such a patch model, as they support investigations of IA violations, based on the source of the violations. These agencies are roughly depicted in Figures 1 and 2. In the models shown, all the agencies are reflected as patches on a grid, or landscape, the lines in the grid reflecting cross-boundary communication channels, as described by Kauffman (264). Each patch is linked in at least one channel to at least one other patch or organization. In order to simplify the current model, only major military services are shown as patches, but in reality there are more distinct agencies. Also, their own interpretations and implementations of IA policy could be included in the model, particularly when it comes to configuration control. Existing interface points are also not modeled, although they could be depicted as well.

The use of patch theory in such a model would allow each of the patches (or organizations / sub-organizations) to seek individual optimization, much like it naturally happens in the real world. The improvements in one organization influences the behaviors of other connected patches, causing global change. The overall organization (e.g., the federal government) is reflected by the

entire grid. Localized optimization influences global optimization, through the interagency process. As one patch optimizes, it causes perturbations that strengthen the likelihood of policy improvement in other agencies, as the other agencies seek to respond to changes that tend to increase fitness.

Experimentation is obviously the key for adaptive, patch-modeled organizations. Agent-based modeling offers such an experimental environment. Experimentation offers the potential for non-deductive inference to emerge. Recall that deduction is a syllogism inferring from a larger body of information to a conclusion that by definition is contained within the premises. While detection of overlooked information may take place, nothing new can be discovered, again by definition. Non-deductive inference, such as induction, allows for inference that transcends the existing body of information. Induction and agent-based modeling allow for true discovery to take place (Axelrod, 1997, 3-4).

The inventor of the genetic algorithm and agent-based modeling pioneer John Holland confirms this thinking in his discussion on classifier systems, an agent-based modeling environment. "It is a central tenet of our approach that all rules serve as hypotheses, more or less confirmed, rather than as incontrovertible facts." Holland notes this idea of rules as hypotheses in describing the value of modeling rules as something to test and challenge rather than as hard and fast dictates of a parent organization (as quoted in White).[25] Mark White expands Holland's thinking into his discussions on adaptive organizations (1997).

Information Assurance rules and regulations are developed and promulgated through federal law and augmented by organizational policy and rules, from centralized sources, as noted above. Extending White's and Holland's ideas about adaptive organizations, as well as their laws and rules, it is practical to consider that policy-makers could improve interagency cooperation about IA (as well as other rules and regulations) by applying testing through agent-based modeling. In fact, rules and regulations could be designed to be adaptive, covering a range of possible outcomes rather than narrowly focused situations.

Through testing and experimentation it is likely that leaders can gain insights about organizational interaction with rules after they are published, and learn the consequences of their actions – in such a case more effective use of deduction could occur and useful determinations of cause-and-effect relationships might reveal themselves. Extending that potential further, it is also likely these same leaders-as-modelers can also better understand potential rule and policy changes to organizations before the rules are implemented. Perhaps all it takes is a willingness to experiment and think of rules as hypotheses and organizations as patches.

One shortcoming of Kauffman's patch model is that it suggested a way to visualize and think about organizations rather than as a way to characterize them. *NK* models, while elegantly suggestive, are abstract visualizations at best. How might a leader-modeler actually build patches such that they reflected her organization? Kauffman hints at one approach easily understood by members of the US government when he compares the United States to a patchwork of 50 patches, but his granularity seems to stop there (270-271). Practical use of patches demands more.

---

[25] Compare to Holland's discussions about rules as hypotheses in Holland, 1995, page 53).

Applying Patches. Consider patches as being composed of agents similar to those that populated the Agent Based Evidence Marshaling model. ABEM agents possess limited understanding of their little piece of their world (their patch). Through interaction, assisted by message-passing schemas such as tuples or Holland's tagged "building block" messages (Holland, 34-40), agents learn from each other. Through substitution and nomination, agents are able to learn or suggest other information that may be important to them. Interaction produces learning, which in turn produces more interactions. Rich, insightful complexity emerges.

Through human intervention and intuition, the inference processes promulgated by ABEM agents suggest to the ABEM user strategically important questions or lines of inquiry to pursue. The leader-modeler re-instantiates relevant ABEM agents with new lines of inquiry, empowers the agents to react to the new information, and visualizes the results. New learning occurs at both the agent and the human user levels. A form of self-organization and self-governance among the agents can emerge.

The notion of self-governance in a high-technology environment is not new. In fact, Johnson and Post describe another interesting potential use of Kauffman patches as a model for constructing cooperative, self-organizing governance for the entire Internet community. They suggest a "federalist decision-making" form of government for the global Internet. Their approach substantiates that physical co-location is hardly necessary for what amounts to anonymous agreement about distributed policy evolution that emerges to be "best" for all concerned (Johnson and Post, 1997).

Kauffman patches, consisting of ABEM-like agents seeking to self-optimize, cause perturbations within the landscape as each patch seeks to increase its own fitness. It may be far more effective and efficient to observe such turmoil within an agent-based modeling environment than in the real world, where resources and even lives may be at stake.

The visual execution of this type of model would allow for decision-makers to observe changes both in individual patches and in various hierarchies of the organizations involved. Discovery of emergent, naturally optimized linkages and cooperation points (interfaces) are possible. It will of course be necessary to develop more specific architectures to support this type of patch-based simulation of emergence, as well as better define the organizations involved. The existing ABEM agents clearly are limited to basic forms of inference, based on simple curiosity at this point. The ABEM architectural groundwork exists, however, and more extensive research is in fact ongoing.

Agent-based models like ABEM can increase the likelihood of success in implementing new policies by providing an experimental laboratory in which to visualize relationships between inputted behaviors and new information, and the outcomes that result from the new or altered inputs. The visualizations are not limited to only the user's intuition, as demonstrated by ABEM agent development, but the self-organizing behaviors of the individual agents interacting among themselves produce emergent global knowledge that the human user may not have previously considered. New lines of inquiry may reveal themselves.

Interfaces between organizations can also appear as emergent phenomena. If it is important to allow for agents to interact and self-organize, it is equally important to allow them to discover efficient means overcome barriers and to communicate. Interfaces are essentially communications portals. Agents that evolve and discover ways around inhibitions of policy and technology mismatches are likely to also find new ways to interface with each other. In this

way, leaders of even divergent organizations may find enhanced capabilities to communicate with each other and learn to cooperate better.

ABEM and patches offer a new way to think about and visualize complex organizations, the interactions of these organizations, and the policy changes that stimulate change throughout. Some complexity is thrust upon leaders and they must simply cope. Other leaders may wish to grow complexity for their own purposes and at their own rate. If complexity is an emergent phenomenon, modeled in ways that transformation points such as phase transitions may be monitored as they are occurring, organizational leaders may be able to better control or at least cope with change.

Introductions of multiple policies, organizational cultures, different types of information technology assets, and the diverse personalities of those responsible to administer Information Assurance policies guarantees complex relationships with which leaders must deal. Until the advent of agent-based modeling techniques it was very difficult to capture the nuances of interaction of components and leaders were often left to scratch their heads in wonderment of how to make so many things work together at the same time. Tools now exist to ease this burden. Patches and Agent Based Evidence Marshaling offer a new way to "cope."

6. Conclusions.

Gareth Morgan notes "Western management, with its enormous emphasis on the achievement of predetermined goals, objectives, and operational targets, overasserts desired *intentions* and underplays the importance of recognizing the *limits* that need to guide behavior," (91). Morgan interweaves important principles of complexity theory into his writing, and his observation clearly points out the difficulties with aggressive all-encompassing planning efforts that ignore the potentials of emergence. As Morgan writes,

> …complexity defies comprehensive analysis, and it is often difficult to know where to intervene…In complex systems, no one is ever in a position to control or design system operations in a comprehensive way. Form emerges. It cannot be imposed and there are no end states. (232-233)

Thinking in terms of complexity and emergence helps leaders understand that end states are an illusion and that total control of system and interagency design cannot be engineered. At best, they can have insights brought about by asking "right questions" that lead to better understanding and appreciation of emerging form. Agent-based modeling provides an insight-producing toolkit that facilitates this understanding.[26]

This paper discusses using agent-based models as a method to apply Kauffman's patch theory to an interagency Information Assurance problem. The patches in the proposed model may be powered by agents similar to those described in the ABEM architecture. Whereas IA discusses protection of critical information technology resources, agent-based models and patch theory can apply to many classes of interagency cooperation issues. The same principle applies to intra-agency challenges, as well. It is basically a matter of "chunking" the problem into the "right" size family of patches and allowing local optimization through empowered agents to influence

---

[26] Although he does not discuss agent-based models overtly, Morgan would likely call the visualizations and insights these models can provide "imaginization" (322).

eventual global optimization. If Kauffman is right, that's how life has solved hard problems since it began.

The organizations described in the drawings above represent just enough diversity to suggest to organizational leaders the challenges of interagency cooperation in coping with difficult and contentious matters such as information assurance in the Department of Defense. The purpose of this paper is to propose new ways of visualizing complex relationships and look for the convergence points where information interactions can lead to self-organizing lines of inquiry to prompt leaders to pursue better questions to ask than simple intuition or single-minded implementing instructions can provide.

Local individual IA leaders can potentially interact within their own patches, optimizing the environment for their own success, following the least complex global rule set feasible. From these local exchanges, the IA patches can find appropriate interface points to stimulate perturbations that extend to other patches. Other patches will be affected by these connections and change themselves, causing more perturbation. Eventually, if modeled effectively, a phase transition that affects the entire organization can take place and transform local levels of fitness toward global increases in fitness.

Patches and ABEM targeted toward difficult interagency cooperation problems can provide emergent solutions that leaders just did not happen to consider when following rigid universally directed regulations. Through model-stimulated suggestion of novel lines of inquiry, new directions for success can emerge. Asking the right questions at least gives the leader the insight to know what she does not know.

Agent-based models allow leaders to gain meaningful and visual insights into the overall problem at hand in order to build a better environment for real-life emergent cooperation. Organizational leaders endure great hardship in defining the real problems their agencies face in the first place. Kauffman's keen insight on learning "how to learn in the face of persistent misspecification" points to the potential value of simulations for emergence models in support of interagency processes. Add to more effective problem definition the potential for discovering in a timely manner emergent solutions that are "good enough," subtract the costs of organizational mistakes from solving the wrong problem, and it appears that agent-based models may be poised to make a worthwhile contribution to the interagency cooperation and decision-making process.

Bibliography

Alberts, David S., Garstka, John J., and Stein, Frederick P., *Network Centric Warfare: Developing and Leveraging Information Superiority*, United States Department of Defense C4ISR Cooperative Research Program, Washington, DC, 1999.

Axlerod, R., *The Complexity of Cooperation*, Princeton University Press, Princeton, NJ, 1997.

Axelrod, R., and Cohen, M., *Harnessing Complexity*, Free Press, NY, 1999.

Baskin, Ken, *Corporate DNA: Learning from Life*, Butterworth-Heinemann Publishers, Boston, 1998.

Cilliers, Paul, "Rules and Complex Systems," *Emergence*, Volume 2, Issue 3, Third Quarter 2000, (http://emergence.org/Emergence/Archivepage.htm), accessed 23 February 2003.

Clark, Richard A., and Schmidt, Howard A., "A National Strategy to Secure Cyberspace," a working draft released for public comment, September, 2002, available at http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html, accessed on 05 January 2003.

Defense-Wide Information Assurance Program Website, located at http://www.c3i.osd.mil/org/sio/ia/diap/, accessed 8 February 2003.

Devlin, Keith J., *The Language of Mathematics*, W. H. Freeman and Company, New York, 1998.

Epstein, J., and Axtell, R., *Growing Artificial Societies*, Brookings Institution Press, Washington, DC, 1996.

Holland, J., *Hidden Order*, Addison-Wesley, Reading, MA, 1995.

Hughes, Frank J., and Schum, David A., *The Art and Science of the Process of Intelligence Analysis*, a text for the Joint Military Intelligence College, Defense Intelligence Agency, Washington, D.C., 2003.

Hunt, Carl W., *Agent Based Evidence Marshaling: Agent-Based Creative Processes for Discovering and Forming Emergent Scenarios and Hypotheses*, Doctoral Dissertation, George Mason University Library, Fairfax, VA, 2001.

Johnson, David R., and Post, David G., "The New 'Civic Virtue' of the Internet," First Monday: A Peer-Reviewed Journal on the Internet, located at: http://www.firstmonday.dk/issues/issue3_1/johnson/#author, accessed on 7 February 2003.

Kauffman, Stuart A., The Origins of Order, Oxford Press, New York, 1993.

Kauffman, Stuart A., *At Home in the Universe*, Oxford Press, New York, 1995.

Kauffman, Stuart A., "Escaping the Red Queen Effect," The McKinsey Quarterly, Number 1, 1995, located at: http://gemini.tntech.edu/~mwmcrae/esre95.html, accessed on 9 February 2003.

Minsky, M., "Commonsense-Based Interfaces", Communications of the ACM, Vol. 43, No. 8, August, 2000.

Morgan, Gareth, *Images of Organization*, Berret-Koehler Publishers, San Francisco, 1998.

Morowitz, Harold K., *The Emergence of Everything*, Oxford Press, New York, 2002.

Morris, Richard, *Artificial Worlds: Computers, Complexity and the Riddle of Life*, Plenum Trade, New York, 1999.

Sanders, T. Irene, *Strategic Thinking and the New Science*, The Free Press, New York, 1998.

Schum, David A. "Marshaling Thoughts and Evidence During Fact Investigation," *South Texas Law Review*, Vol. 40, No. 2, Summer, 1999.

Title 18, United States Code, Chapter 47, Section 1030, http://www4.law.cornell.edu/uscode/18/1030.html and http://frwebgate4.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=79589628194+0+0+0&WAISaction=retrieve, accessed 05 January 2003.

Title 40, United States Code, Chapter 25, Section 1441, http://www4.law.cornell.edu/uscode/40/ch25.html and http://frwebgate4.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=79589628194+4+0+0&WAISaction=retrieve, accessed 05 January 2003.

United States Critical Infrastructure Protection Office, "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May, 1998, http://www.ciao.gov/publicaffairs/pdd63.html, accessed on 22 February 2003.

United States Department of Homeland Security Government Website, located at http://www.whitehouse.gov/deptofhomeland/, accessed on 05 January 2003.

United States Department of Justice, DOJ Press Release: "London, England Hacker Indicted Under Computer Fraud and Abuse Act For Accessing Military Computers," dated 12 November 2003, located at http://www.usdoj.gov/criminal/cybercrime/mckinnonIndict.htm, accessed on 22 February 2003.

White, Mark, "Adaptive Corporations," located at: http://www.geocities.com/wallstreet/7891 (accessed on 9 April 2003), Mark White and Associates, Mexico City, Mexico, 1997.